Symantec
A Division of Broadcom

Producto breve

Prevención de pérdida de datos de Symantec®

Impulse la protección total de sus datos confidenciales

El más alto nivel de protección de datos

- La protección de datos más amplia para los canales de comunicación: nube, correo electrónico, web, terminales y almacenamiento.
- Menos falsos positivos con tecnologías de detección integrales.

Un solo panel de vidrio

- Una única consola para la gestión de políticas, respuesta a incidentes, informes y administración.
- Un conjunto de políticas y flujo de trabajo para todos los canales de comunicación: nube, correo electrónico, web, terminales y almacenamiento.

Una amplia gama de integraciones

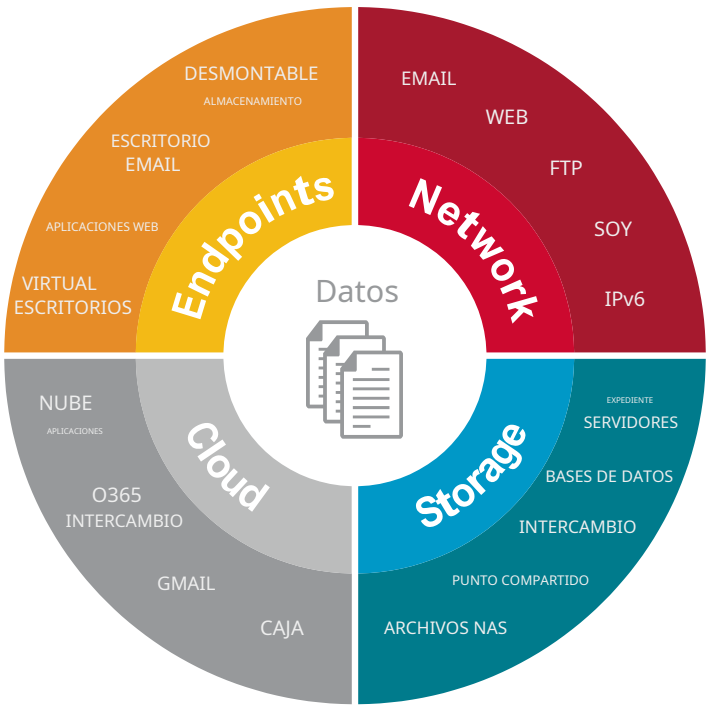
- Parte de Symantec Enterprise Cloud que admite un sistema centrado en datos, Visión SASE habilitada para híbridos.
- Totalmente integrado con Microsoft Information Protection para clasificación de datos, cifrado y gestión de derechos.

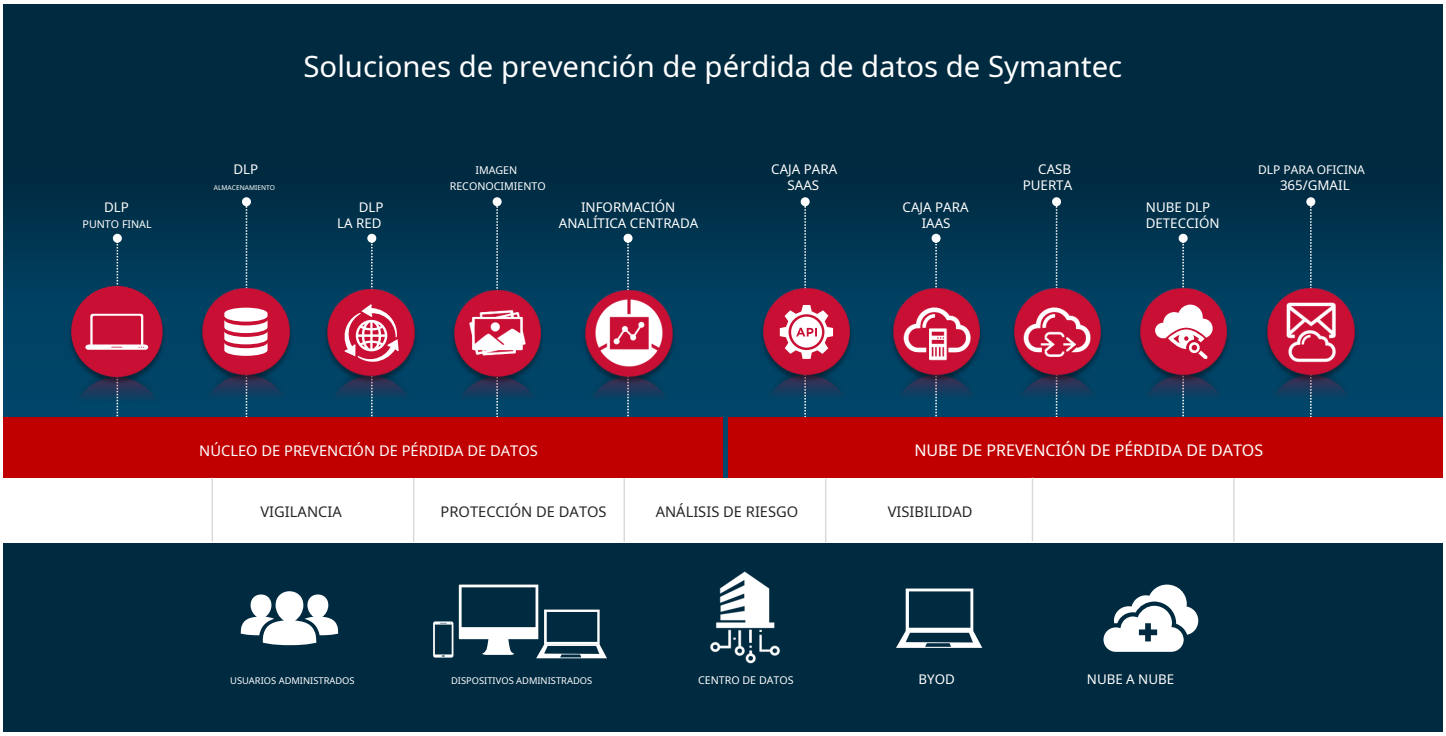
Detenga la pérdida de datos con el más alto nivel de protección

Mantener la información segura y en conformidad nunca ha sido fácil. Pero hoy en día, las empresas enfrentan problemas de seguridad nuevos e inesperados. A medida que más empresas desconectan sus sistemas locales y pasan a servicios basados en la nube, los datos de la empresa se vuelven más vulnerables a la exposición accidental por parte de usuarios de la nube sin experiencia y errores de configuración. La seguridad en la nube no es la única preocupación para las empresas: los ataques cibernéticos dirigidos se han vuelto demasiado comunes a medida que los ciberdelincuentes desarrollan nuevos métodos efectivos que eluden las medidas de seguridad tradicionales y explotan a los usuarios para robar datos valiosos de las empresas.

La solución Symantec Data Loss Prevention (DLP) ofrece el más alto nivel de protección necesario para evitar filtraciones de datos y salvaguardar la reputación de su empresa. Con nuestra tecnología líder en la industria, obtiene capacidades integrales de descubrimiento, monitoreo y protección que le brindan visibilidad y control total sobre sus datos confidenciales.

- Descubra dónde residen los datos en todos los canales: nube, correo electrónico, web, terminales y almacenamiento
- Supervisar cómo se utilizan los datos dentro y fuera de la red corporativa
- Proteja los datos para que no sean expuestos o robados en tiempo real





Una forma sencilla de obtener la cobertura que necesita

Symantec DLP está disponible en dos conjuntos de soluciones: DLP Core y DLP Cloud. Juntos brindan protección de seguridad de la información de clase mundial en puntos finales, red, nube y almacenamiento. DLP Core incluye protección para terminales, redes y ubicaciones de almacenamiento, al tiempo que ofrece reconocimiento de imágenes confidenciales y análisis centrado en la información (análisis de comportamiento de entidades de usuario). DLP Cloud permite que las políticas de DLP se extiendan a entornos de nube al proporcionar controles completos de CASB junto con conectores de nube DLP para puertas de enlace web y de correo electrónico.

Mantenga los datos seguros mientras están en uso en los puntos finales

A medida que los empleados se vuelven más móviles mediante el uso de computadoras portátiles, los datos de la empresa se vuelven más vulnerables a las filtraciones y robos de datos, tanto dentro como fuera de la red corporativa. La solución Symantec DLP for Endpoint (proporcionada con DLP Core) proporciona toda la protección necesaria para mantener los datos confidenciales seguros y protegidos en los puntos finales. Brinda capacidades completas de detección, monitoreo y protección para los datos en uso en una amplia gama de canales: correo electrónico, aplicaciones en la nube, protocolos de red, almacenamiento externo y servidores y escritorios virtuales. Con Symantec DLP, un único agente ligero para endpoints habilita dos módulos: DLP Endpoint Discover y DLP Endpoint Prevent.

- Descubrimiento de Symantec DLP Endpointescanea los discos duros locales y le brinda una visibilidad profunda de los archivos confidenciales que los usuarios almacenan en sus computadoras portátiles y de escritorio. Proporciona una amplia gama de respuestas, incluida la cuarentena de archivos local y remota, el cifrado basado en políticas y la administración de derechos digitales habilitados por la API DLP Endpoint FlexResponse.
- Prevención de Symantec DLP Endpointsupervisa las actividades de los usuarios y le brinda un control detallado sobre una amplia gama de aplicaciones, dispositivos y plataformas. Proporciona una amplia gama de respuestas, incluido el cifrado basado en la identidad y los derechos digitales para los archivos transferidos a USB. Con Endpoint Prevent, puede alertar a los usuarios sobre incidentes mediante ventanas emergentes en pantalla o notificaciones por correo electrónico. Los usuarios también pueden anular las políticas proporcionando una justificación comercial o cancelando la acción (en el caso de un falso positivo).

punto final	Disponibilidad
navegadores	cromo | safari | Firefox | IE y borde
Aplicaciones en la nube	Caja | Dropbox | Unidad de Google | microsoft onedrive
Aplicaciones de correo electrónico	Perspectiva | notas de loto
Protocolos de red	HTTP | HTTPS | FTP
Almacenamiento extraíble	dispositivos MSC | dispositivos MTP
Escritorios virtuales	Citrix | Microsoft Hyper-V | vmware
Otros	Imprimir | fax | Compartir red | Portapapeles

Proteja los datos en movimiento a través de la red

La adopción generalizada de herramientas de colaboración y aplicaciones en la nube, junto con el comportamiento arriesgado de los empleados del que las empresas ni siquiera pueden ser conscientes, aumenta el riesgo de exposición de datos en las comunicaciones comerciales. La solución Symantec DLP for Network (proporcionada con DLP Core) supervisa y evita que se filtren datos confidenciales a través de una amplia gama de protocolos de comunicación en su red.

DLP Network Monitor captura y analiza el tráfico saliente en su red corporativa y detecta contenido confidencial y metadatos sobre protocolos estándar, no estándar y propietarios. Se implementa en los puntos de salida de la red y se integra con su red tap o Switched Port Analyzer (SPAN). Network Monitor realiza una inspección profunda del contenido de todas las comunicaciones de la red sin pérdida de paquetes, a diferencia de otras soluciones que muestrean los paquetes durante los picos de carga y lo ponen en alto riesgo de falsos negativos.

DLP Network Prevent for Email protege los mensajes confidenciales para que no sean filtrados o robados por empleados, contratistas y socios. Supervisa y analiza todo el tráfico de correo electrónico corporativo y, opcionalmente, modifica, redirige o bloquea los mensajes en función del contenido confidencial u otros atributos del mensaje. Network Prevent for Email se implementa en puntos de salida de la red y se integra con agentes de transferencia de correo (MTA) y correo electrónico basado en la nube, incluido Microsoft Office 365 Exchange. Network Prevent for Email está disponible como software o dispositivo virtual.

DLP Network Prevent for Web protege los datos confidenciales para que no se filtren a la web. Supervisa y analiza todo el tráfico web corporativo y, opcionalmente, elimina el contenido HTML confidencial o bloquea las solicitudes. Network Prevent for Web se implementa en los puntos de salida de la red y se integra con su servidor proxy HTTP, HTTPS o FTP mediante ICAP. Network Prevent for Web está disponible como software, dispositivo de hardware o dispositivo virtual.

Proteja los datos en reposo en los repositorios de almacenamiento

Los datos digitales están creciendo significativamente, en gran parte debido a los documentos generados internamente, pero pocas empresas se centran en gobernarlos y protegerlos. Con Symantec DLP for Storage (incluido en DLP Core), puede descubrir y proteger datos confidenciales en reposo: los datos almacenados en servidores de archivos, terminales, almacenamiento en la nube, recursos compartidos de archivos de red, bases de datos, SharePoint y otros repositorios de datos.

Repositorio	Disponibilidad
Servidores de archivos	Windows a través de CIFS y DFS | Unix a través de NFS | Ventanas locales | Unix local (Linux, AIX y Solaris) | Archivadores NAS
Máquinas distribuidas	Portátiles | Escritorios
Documento y correo electrónico Repositorios	SharePoint | Enlace en vivo | Documento | notas de loto | Microsoft Exchange | hora del Pacífico
Contenido web y Aplicaciones	Sitios Web Corporativos | Intranet | Extranet | Aplicaciones personalizadas
bases de datos	oráculo | microsoft | ibmdb2

En primer lugar, Symantec DLP Network Discover encuentra datos confidenciales mediante el análisis de recursos compartidos de archivos de red, bases de datos y otros repositorios de datos empresariales. Esto incluye sistemas de archivos locales en servidores Windows, Linux, AIX y Solaris; bases de datos de Lotus Notes y SQL; y servidores Microsoft Exchange y SharePoint. DLP Network Discover reconoce más de 330 tipos de archivos diferentes, incluidos tipos de archivos personalizados, en función de la firma binaria del archivo. También proporciona escaneo de alta velocidad para entornos grandes y distribuidos y optimiza el rendimiento al escanear solo archivos nuevos o modificados.

Luego, Symantec DLP Network Protect agrega sólidas capacidades de protección de archivos además de Network Discover. Network Protect limpia y protege automáticamente todos los archivos expuestos que Network Discover detecta y ofrece una amplia gama de opciones de reparación, que incluyen poner en cuarentena o mover archivos, copiar archivos en un área de cuarentena o aplicar políticas de cifrado basado en identidad y derechos digitales a archivos específicos. Network Protect incluso educa a los usuarios comerciales sobre las infracciones de las políticas al dejar un archivo de texto de marcador en la ubicación original del archivo para explicar por qué se puso en cuarentena.

Symantec DLP también incluye una plataforma de API FlexResponse que le permite crear acciones personalizadas de reparación de archivos. FlexResponse proporciona una fácil integración llave en mano con otras soluciones de seguridad de archivos de Symantec y de terceros, incluidos Symantec File Share Encryption y Adobe LiveCycle.

Proteja los datos en la nube

Las preocupaciones de seguridad persisten a medida que las empresas continúan migrando aplicaciones de TI heredadas a servicios de nube pública donde es difícil obtener el mismo nivel de visibilidad y control de datos confidenciales que en sus propios servidores privados. Con Symantec DLP Cloud, puede extender potentes controles de protección de datos a la nube con la comodidad de DLP entregado en la nube. Proporciona ricas capacidades de descubrimiento, monitoreo y protección para una amplia gama de aplicaciones en la nube, así como aplicaciones locales.

Protección de datos en la nube (continuación)

El servicio de detección en la nube de Symantec DLP inspecciona el contenido extraído de las aplicaciones en la nube y el tráfico web y aplica automáticamente políticas de datos confidenciales. Ofrece una integración mejorada de nube a nube con Symantec CloudSOC, nuestra solución de agente de seguridad de acceso a la nube líder en la industria, para proteger los datos en movimiento y los datos en reposo en más de 100 aplicaciones en la nube autorizadas y no autorizadas, como Office 365, G-Suite, Caja, Dropbox y Salesforce. La integración permite la extensión a las políticas existentes y una detección robusta a las aplicaciones en la nube, administrando todos los incidentes desde la consola DLP. Los controles incluyen dejar de compartir archivos confidenciales, ponerlos en cuarentena, bloquearlos para que no abandonen la aplicación y también aplicar cifrado basado en identidad y derechos digitales automáticamente a archivos específicos compartidos con terceros.

Symantec DLP Cloud incluye soporte para correo electrónico, lo que permite un monitoreo preciso y en tiempo real del tráfico de correo electrónico corporativo al aprovechar la inteligencia integrada y las capacidades de detección avanzadas que minimizan los falsos positivos. También brinda protección en tiempo real contra fugas de datos con el bloqueo de mensajes automatizado o la modificación de mensajes para aplicar el cifrado o la cuarentena posteriores. Cuando los datos se comparten con terceros, pueden habilitar automáticamente el cifrado basado en la identidad y los derechos digitales para los cuerpos y archivos adjuntos de los correos electrónicos. El servicio DLP en la nube para correo electrónico es compatible con Gmail for Work, Microsoft Office 365 Exchange Online y Microsoft Exchange Server. Está disponible de forma independiente o se puede combinar con las capacidades superiores de protección contra amenazas de correo electrónico del servicio Symantec Email Security.cloud.

Administre desde un solo panel de vidrio

A medida que sus datos se propagan a través de una gama más amplia de dispositivos y entornos de almacenamiento, la capacidad de definir y aplicar políticas de manera consistente se vuelve aún más crítica. Symantec DLP le brinda una consola de administración unificada, la plataforma DLP Enforce, que le permite escribir políticas una vez y luego aplicarlas en todas partes, en todos los canales de pérdida de datos.

Con la plataforma DLP Enforce:

- Use una única consola basada en web para crear políticas de pérdida de datos, remediar incidentes y realizar la administración del sistema en todos sus terminales, dispositivos móviles, servicios basados en la nube y redes y sistemas de almacenamiento locales.
- Aproveche las más de 70 plantillas de políticas predefinidas y un generador de políticas conveniente para poner su sistema en funcionamiento rápidamente.
- Aprovechar las sólidas capacidades de remediación y flujo de trabajo para agilizar y automatizar los procesos de respuesta a incidentes para entornos de alto tráfico.
- Aplique la inteligencia comercial a sus esfuerzos de reducción de riesgos con una herramienta de análisis sofisticada, Symantec IT Analytics for DLP, que brinda funciones avanzadas de generación de informes y análisis ad-hoc.

Obtenga una visibilidad inigualable de los datos confidenciales

El núcleo de cualquier solución DLP es la detección consciente del contenido. Las técnicas de detección de contenido permiten encontrar datos confidenciales almacenados en prácticamente cualquier ubicación y formato de archivo. Symantec DLP ofrece la detección más completa con aprendizaje automático avanzado, reconocimiento de imágenes, huellas dactilares y tecnologías de descripción que clasifican con precisión los datos para que no tenga que preocuparse por los falsos positivos y el impacto en los usuarios empresariales.

- Coincidencia de contenido descritodetecta contenido buscando coincidencias en palabras clave específicas, expresiones regulares o patrones y propiedades de archivo. Symantec DLP proporciona más de 130 identificadores de datos listos para usar, que son algoritmos predefinidos que combinan coincidencia de patrones con inteligencia integrada para evitar falsos positivos.
- Coincidencia exacta de datosdetecta datos tomando huellas dactilares o indexando fuentes de datos estructurados como bases de datos, servidores de directorio y otros archivos de datos estructurados.
- Coincidencia de documentos indexadosaplica métodos de huellas dactilares para detectar datos almacenados en documentos no estructurados, incluidos los documentos de Microsoft Office; PDF; y archivos binarios como JPEG, diseños CAD y archivos multimedia. IDM también detecta contenido "derivado", como texto que se ha copiado de un documento de origen a otro archivo.

- Reconocimiento de imágenes sensibles (proporcionado con DLP Core) detecta texto incrustado en imágenes como formularios escaneados, documentos, capturas de pantalla, imágenes y archivos PDF aprovechando nuestra tecnología patentada de reconocimiento de formularios y caracteres ópticos incorporados.
  Motor de reconocimiento (OCR).
- Aprendizaje automático de vectoresprotege la propiedad intelectual con características matizadas que son raras o difíciles de describir, como los informes financieros y el código fuente. A diferencia de otras tecnologías de detección, Vector Machine Learning no requiere que localice, describa o tome las huellas digitales de los datos que necesita proteger.

Symantec DLP también ofrece un amplio conjunto de API listas para usar y complementarias que le permiten personalizar e integrarse con una amplia gama de productos de seguridad de terceros, nube y aplicaciones propietarias: DLP REST API, DLP FlexResponse API, API de extracción de contenido de DLP, API de actualización e informes de incidentes de DLP y dispositivo virtual de detección de API de DLP.

Extienda la protección de datos más allá de DLP

A medida que los datos confidenciales se comparten con usuarios externos o viajan a la nube y salen de su entorno administrado, se vuelven vulnerables a una exposición no deseada. Nuestra solución brinda protección integral para sus datos a lo largo de su ciclo de vida más allá de sus instalaciones administradas, con seguridad de acceso a la nube basada en políticas, clasificación, encriptación, análisis de usuarios y puertas de enlace web.

- Extienda las políticas de DLP a las aplicaciones en la nube:Extienda la detección, las políticas y los flujos de trabajo de DLP a las aplicaciones en la nube a través de la integración con Symantec CloudSOC (CASB) y administre incidentes en una sola consola.
- Simplifique la clasificación de incidentes y la gestión de políticas: Reduzca el tiempo y los esfuerzos para la corrección de incidentes y la gestión de políticas, y mitigue el riesgo de datos con Symantec Information Centric Analytics (ICA), un análisis de comportamiento de usuarios y entidades proporcionado con DLP Core.
- Comparta datos de forma más segura con otros:Evite el acceso no autorizado a datos confidenciales a través de una autenticación sólida cuando los datos se comparten con socios comerciales con Symantec VIP Identity and Access Management
- Evite que los datos vayan a sitios no deseados:Asegúrese de que los datos confidenciales no se filtren a través del tráfico web no confiable, incluso el tráfico cifrado, aprovechando la integración de DLP con Symantec Secure Web Gateways: Symantec ProxySG y Web Security Service.
- Integrado con Microsoft Information Protection (MIP): Symantec DLP está integrado con las amplias funciones de clasificación y cifrado proporcionadas por MIP. Esta solución brinda a los clientes la capacidad de detectar y leer documentos y correos electrónicos protegidos mediante MIP.

Requisitos del sistema

La solución Symantec DLP comprende una única plataforma de administración unificada, un agente de endpoint liviano y potentes productos de detección de contenido. Ofrecemos la mayor flexibilidad de implementación con una amplia gama de opciones para cualquier tipo de entorno: software local; aparatos virtuales y físicos; servicios de nube pública, privada e híbrida; y servicios gestionados proporcionados por Symantec Partners. A diferencia de otras soluciones, se ha comprobado que Symantec DLP funciona en entornos altamente distribuidos y se amplía a cientos de miles de usuarios.

Para conocer los requisitos completos del sistema de Symantec Data Loss Prevention, visite nuestra página de soporte.

Comience a proteger su información hoy

Symantec está listo para ayudarlo a extender sus políticas de seguridad y cumplimiento más allá de los límites de su firewall, para que pueda descubrir, monitorear y proteger su información de manera más completa y efectiva. Le ofrece el costo total de propiedad más bajo, con metodologías de implementación comprobadas, políticas intuitivas y herramientas de administración de incidentes, y una cobertura integral en todos sus canales de alto riesgo.

Descubra las ventajas de una solución integral de protección de la información creada para el mundo móvil centrado en la nube de hoy:Obtenga más información sobre la prevención de pérdida de datos de Symantec.

Symantec™
A Division of Broadcom

Para más información del producto:broadcom.com